E-mail spams

The OECD has published a toolkit on how to legislate to deal with spam. Explain the extent to which the Unsolicited Electronic Messages Act 2007 meets the suggestions in Element One of the OECD toolkit on spam and analyse the policy reasons for any differences between the Act and the toolkit.

In acknowledgment of the proliferation of communication technologies facilitating the socio-economic problems created by spam, the Joint ICCP-CCP Task Force on Spam was created to " assist in the further conduct and co-ordination on spam and obtain a more rapid consensus on a policy framework to tackle spam issues" (OECD., 2006, p. 2) The task force on Spam was approved by the OECD and resulted in the OECD Anti-Spam Toolkit.

The OECD's drive against spam resulted in the New Zealand Department of Internal Affairs implementing the Unsolicited Electronic Messages Act 2007 (the Act), which came into effect on the 5th September 2007. The focus of this analysis is to review how far the Act has gone to implement the recommendations in Element 1 of the OECD Anti-Spam toolkit.

Element 1 of the OECD toolkit on spam addressed regulatory approaches to tackle spam. Element 1 extrapolates that " the development of anti-spam legislation which tackles spam and related problems is fundamental" (OECD, 2006, p8). Moreover, Element 1 observed: " as the legal, political and cultural environments of different countries vary, there is not a global uniform approach to spam or a common definition of spam accepted at the international level. For this reason the Toolkit, rather than advocate a single approach, aims to underline decision points that need to be discussed while elaborating anti-spam legislation and examine the related policy questions"

(OECD, 2006, p. 24).

Additionally, the Element 1 of the OECD toolkit asserts that in order to be effective, any national anti-spam regulation must achieve the following:

“ 1) To preserve the benefits of electronic communications by increasing user trust in electronic messaging media and improve the availability and reliability;

2) To prohibit and take action against the action of spamming, as defined by national law;

3) To reduce the amount of “ spam” (OECD, 2006, p. 24).

In order to achieve these goals, Element 1 of the toolkit proscribed that legislation should conform to four general principles, namely policy direction, regulatory simplicity, enforcement effectiveness and international linkages (OECD, 2006, p. 25).

The central purposes of the Act are set out below:

1) To prohibit unsolicited commercial electronic messages (defined as spam) with a New Zealand link.

2) Require commercial electronic messages to include accurate information about the person who authorised the sending of the message and a functional unsubscribe facility to enable the recipient to instruct the sender that no further messages are sent to the recipient;

3) Prohibit address-harvesting software being used to create address lists for sending unsolicited commercial electronic messages; and

4) Deter people from using information and communication technologies inappropriately.

The Act further aims to encourage consistent direct marketing practices by requiring electronic messages to include an unsubscribe facility and ensure

that electronic messages are only sent to customers who have consented to receiving it (New Zealand Department of Internal Affairs, 2007, p. 4).

If we consider the central provisions of the Act in context of Element 1 of the OECD toolkit, the underlying aims of the Act are clearly in line with the objectives of the Regulatory framework as set out in Element 1.

Additionally, as highlighted above, Element 1 set out four general principles that national legislation should conform to in implementation. The first principle relates to policy direction and asserts: “ the legislation should provide a clear policy direction. The main lines and objectives of national and international anti-spam policy should be outlined at an earlier stage” (OECD, 2006, p. 24); which is clearly reflected in the spirit of the Act.

Secondly, Element 1 asserted the importance of enforcement effectiveness, by stating: “ it is important to put in place an effective sanction regime and appropriate standards of proof” (OECD, 2006 p. 25). Indeed, the staggering pace of Internet growth has compounded the inherently problematic concept of privacy protection by the proliferation of spam communications. This new medium has widened the scope of information dissemination and communication at social level at a rate beyond original predictions. However, the inherent drawback of the technological revolution is the ease and low cost of information dissemination, coupled with the shield of anonymity, rendering protection against spam increasingly problematic (Ian Lloyd, 2004).

If we consider enforcement procedures under the Act, the Department of Internal Affairs is responsible for enforcement by the following methods:

1) Investigating complaints regarding spam;

2) Acting against “ spammers” who are deliberately flouting the law.

3) Undertaking research into technologies used to send spam;

4) Liaising with relevant overseas bodies to ensure cross-border compliance (New Zealand Department of Internal Affairs, 2007).

Additionally, Business and individuals are able to institute complaints about spam with the “ Anti-Spam Compliance Unit” (New Zealand Department of Internal Affairs, 2007). The Act specifies a number of penalties available to enforce infringement of its provisions, including formal warnings, infringement notices and court proceedings. Furthermore, any business found in breach of the Act is exposed to the potential of a court-imposed fine of up to $500, 000.

Moreover, a business could also be liable to pay compensation to a victim up to the amount of loss suffered or damages up to the amount of profit that was made as a result of sending the spam under the Act. To this end, the Act clearly follows the sentiment of Element 1 that “ enforcement is a fundamental issue, which, if not dealt with appropriately, can make a good piece of legislation useless” (OECD, 2006 p. 25).

The variety of sanctions available under the Act for enforcement operates as a deterrent to infringement. However, the effectiveness of any sanctions is inherently dependent on the Department of Internal Affairs being proactive in applying the principles of the Act in practice. Accordingly, whilst the enforcement provisions of the Act clearly implement the regulatory objectives of the OECD toolkit, it remains to be seen how far this will be implemented in practice.

Finally, Element 1 asserted the importance of transnational initiatives and co-operation to combat spam and provided that any legislation “ should foresee appropriate international linkages, and provide national authorities

with the possibility to co-operate in investigations and exchange information with foreign authorities" (OECD, 2006, p. 25). As stated above, part of the Act's enforcement procedure and policy expressly states the need to ensure compliance and effective liaison with overseas bodies to ensure cross-border compliance.

The Act was implemented in September 2007 and as such, it remains too early to conclude how far it has gone to successfully implement the recommendations of the OECD toolkit. With regard to the regulatory framework recommendations under Element 1, the Act's provisions theoretically supports the recommendations of the toolkit, particularly by implementing numerous sanctions for infringement. However, the Department of Internal Affairs controls enforcement action. Accordingly, the success of the Act in implementing the OECD recommendations inherently depends on consistent and proactive enforcement action in practice.

Bibliography

Ian Lloyd (2004). Information Technology Law. 4th Edition Oxford University Press.

Organisation for Economic Co-operation and Development (2006). Task Force on Spam: Report of the OECD Task Force on Spam: Anti-Spam toolkit of recommended policies and measures. Available at www. oecd. org

Department of Internal Affairs (2007). Unsolicited Electronic Messages Act 2007: Prohibiting Spam and Promoting Good Business Practice. Available at www. dia. govt. nz

Unsolicited Electronic Messages Act 2007. Available at www. legislation. govt. nz/act/public/2007/0007/latest/DLM405134. html